

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1 1. (Currently Amended) A method of windowed backward key generation, comprising:  
2 [[a)]] providing, by a computer system, information to a user that allows determining a  
3 limited number of previous keys in a series of keys from a later key in the series ~~and wherein~~  
4 ~~said information is derived from at least one of said limited number of previous key in said~~  
5 ~~series;~~  
6 [[b)]] generating, by the computer system, a key in the series, based at least in part on  
7 said information provided to said user;  
8 [[c)]] providing, by the computer system, said generated key in the series to the user[[:  
9 and]] to allow a determination of  
10 d) ~~said user determining~~ at least one key in the limited number of previous keys in  
11 the series by applying said information to said generated key in the series ~~provided to the user.~~

1 2. (Currently Amended) The method of Claim 1, wherein [[said a)]]providing the  
2 information comprises providing a key rotation element that is forward rotatable by said user but  
3 is not backward rotatable.

1 3. (Currently Amended) The method of Claim 1, wherein [[said a)]]providing the  
2 information comprises providing to the user a key rotation exponent that is used to determine a  
3 previous key in the series from a later key in the series by exponentiating said later key by said  
4 key rotation exponent.

1 4. (Currently Amended) The method of Claim 2, further comprising:  
2 [[e1)]] generating, from the key rotation element, a new key rotation element;  
3 [[e2)]] generating a new key based, in part, on said new key rotation element; and  
4 [[e3)]] distributing said new key to non-revoked users.

1 5. (Currently Amended) The method of Claim 1, wherein ~~said a)~~ further providing the  
2 information comprises providing a secret share and a key rotation catalyst to said user, wherein  
3 said secret share and said key rotation catalyst allow said user to generate a next key in the series  
4 provided sufficient public information is available.

1 6. (Currently Amended) The method of Claim 5, further comprising:  
2 [[e)] publishing at least one public share, wherein the next key in the series is  
3 determinable based on the key rotation catalyst, the secret share, and the at least one public  
4 share.

1 7. (Original) The method of Claim 5, further comprising revoking a user by publishing a  
2 version of the revoked user's secret share.

1 8. (Currently Amended) A method of windowed backward key rotation, comprising:  
2 [[a)] providing, by a computer system, to a user a key rotation element and a key ( $K_i$ ),  
3 wherein later versions of the key rotation element are determinable ~~by the user using a~~  
4 predetermined function but previous versions of the key rotation element are not determinable ~~by~~  
5 ~~said user using the predetermined function;~~  
6 [[b)] generating, by the computer system, a later version of the key ( $K_{i+n}$ ) based on a  
7 later version of the key rotation element, wherein "n" is a positive integer;  
8 [[c)] providing, by the computer system, to the user the later version of the key ( $K_{i+n}$ )[[;  
9 and]] to allow a determination of  
10 d) ~~said user determining~~ a particular version of the key from ( $K_i$ - $K_{i+n-1}$ ), inclusive, by  
11 applying a version one of the later versions of the key rotation element to a given version of the  
12 key from ( $K_{i+1}$ - $K_{i+n}$ ), inclusive, wherein the given version of the key is a later version than the  
13 particular version of the key.

1 9. (Currently Amended) The method of Claim 8, ~~wherein said d) comprises~~further  
2 comprising:

3 [[d1]] ~~said user~~ determining a later version of said key rotation element from said  
4 provided key rotation element ~~provided in said a).~~

1 10. (Currently Amended) The method of Claim 9, wherein ~~said d)~~ further comprises:

2 [[d2]] ~~said user~~ determining the version of the key  $K_{i+n-1}$  is performed by applying the  
3 one of the later versions ~~version~~ of the key rotation element to the version of the key  $K_{i+n}$ .

1 11. (Currently Amended) The method of Claim 8, further comprising:

2 [[e1]] generating a new key rotation element;

3 [[e2]] generating a new key based, in part, on said new key rotation element; and

4 [[e3]] distributing said new key to non-revoked users.

1 12.-14. (Cancelled)

1 15. ((Currently Amended) A method of windowed backward file key generation, comprising:

2 [[a]] generating, by a computer system, ~~an initial~~ a file key;

3 [[b]] generating, by the computer system, a ~~an initial~~ key rotation exponent, wherein

4 said ~~initial~~ key rotation exponent allows previous versions of the file ~~key~~ key to be

5 determined, wherein a first previous version of the file key is computable from the generated file

6 key and the generated key rotation exponent, and a second previous version of the file key earlier

7 than the first version is computable from the first previous version of the key file and a previous

8 version of the key rotation exponent ~~back until a pre-determined version of the file key, but no~~

9 ~~file keys further back; and~~

10 e) ~~providing said initial file key and said initial key rotation exponent to initial users.~~

1 16. (Currently Amended) The method of Claim 15, further comprising:

2 [[d]] joining a new user by distributing said ~~[[new]]~~ generated file key and said

3 ~~[[new]]~~ generated key rotation exponent to said new user.

- 1 17. (Currently Amended) The method of Claim 15, further comprising:  
2 [[d1))] generating a new key rotation exponent;  
3 [[d2))] generating a new file key based, in part, on said new key rotation exponent; and  
4 [[d3))] distributing said new file key to non-revoked users.
- 1 18. (Cancelled)
- 1 19. (Currently Amended) The method of Claim 15, wherein further comprising:  
2 ~~said a) further comprises~~ generating a key rotation catalyst; and  
3 ~~said e) further comprises~~ providing a secret share and said key rotation catalyst ~~to ones of~~  
4 ~~said initial users~~, wherein said secret share and said key rotation catalyst allow ~~said initial users~~  
5 ~~to generate~~ generation of a new version of the file key provided sufficient public information is  
6 available.
- 1 20. (Currently Amended) The method of Claim 19, further comprising:  
2 [[d))] publishing a public share, wherein ~~said initial~~ users are able to determine a new  
3 version of the file key using their own secret shares, the public shares, the key rotation catalyst,  
4 and a previous file key.
- 1 21. (Currently Amended) The method of Claim 19, further comprising:  
2 [[d1))] generating a new key rotation catalyst;  
3 [[d2))] publishing said new key rotation catalyst;  
4 [[d3))] generating a new file key based, in part, on said new key rotation catalyst; and  
5 [[d4))] publishing a revoked user's private share.
- 1 22. (New) The method of Claim 8, wherein the predetermined function is a one-way hash  
2 function.